An Example of Risk Informed Design

May 9, 2014

Rick Banke – SAIC
Warren Grant – NASA
Paul Wilson - SAIC

Outline

- Description of Risk Informed Design
  - Definition of Risk
- Simple Case Study

Risk Definition

- Risk is operationally defined as a set of triplets[1]:
  - The *scenario(s)* leading to degraded performance with respect to one or more performance measures (e.g., scenarios leading to injury, fatality, destruction of key assets; scenarios leading to exceedance of mass limits; scenarios leading to cost overruns; scenarios leading to schedule slippage).
  - The *likelihood(s)* (qualitative or quantitative) of those scenarios.
  - The *consequence(s)* (qualitative or quantitative severity of the performance degradation) that would result if those scenarios were to occur.

[1]NASA Risk-Informed Decision Making Handbook, NASA/SP-2010-576, Version 1.0, April 2010

Risk-Informed Design

An approach that allows for a system designer to understand and account for the probability of some undesired outcome and the scenarios or failures that would cause that outcome given a specific design

- Allows for Risk-Informed Decision Making
- Allows risk to be “traded” with other design commodities, such as mass, schedule, cost, etc.
- Ideal for design comparison studies

Definitions

- Define LOC & LOM[2]:
  - LOC – Death of or permanently debilitating injury to one or more crew members.
    - Generally assume that loss of entire subsystem function would constitute LOC
  - LOM – Loss of or inability to complete significant/primary mission objectives, including LOC.
    - Trickier to define as dependent upon subsystem capabilities, operations, and procedures
    - In design phase these are often poorly defined/understood
    - Fall-back position is “LOM = 1 failure removed from LOC”
  - LOM_O = LOM – LOC

[2]Multi-Purpose Crew Vehicle Program Probabilistic Risk Assessment (PRA) requirements Document, Rev B, MPCV 70017

Case Study

- NASA Engineering requested a Loss of Crew (LOC) & Loss of Mission (LOM) analysis of a particular system design.
  - Primarily concerned about the baseline system's ability to control internal fluid leakage
    - Isolation valves provided to protect against such leakage would render ½ of the system useless
    - Leakage of any single valve would lead to Loss of Mission
  - Had proposed an alternative design that would permit isolation of pairs of components
  - Second design alternative proposed that would permit pair and string isolation

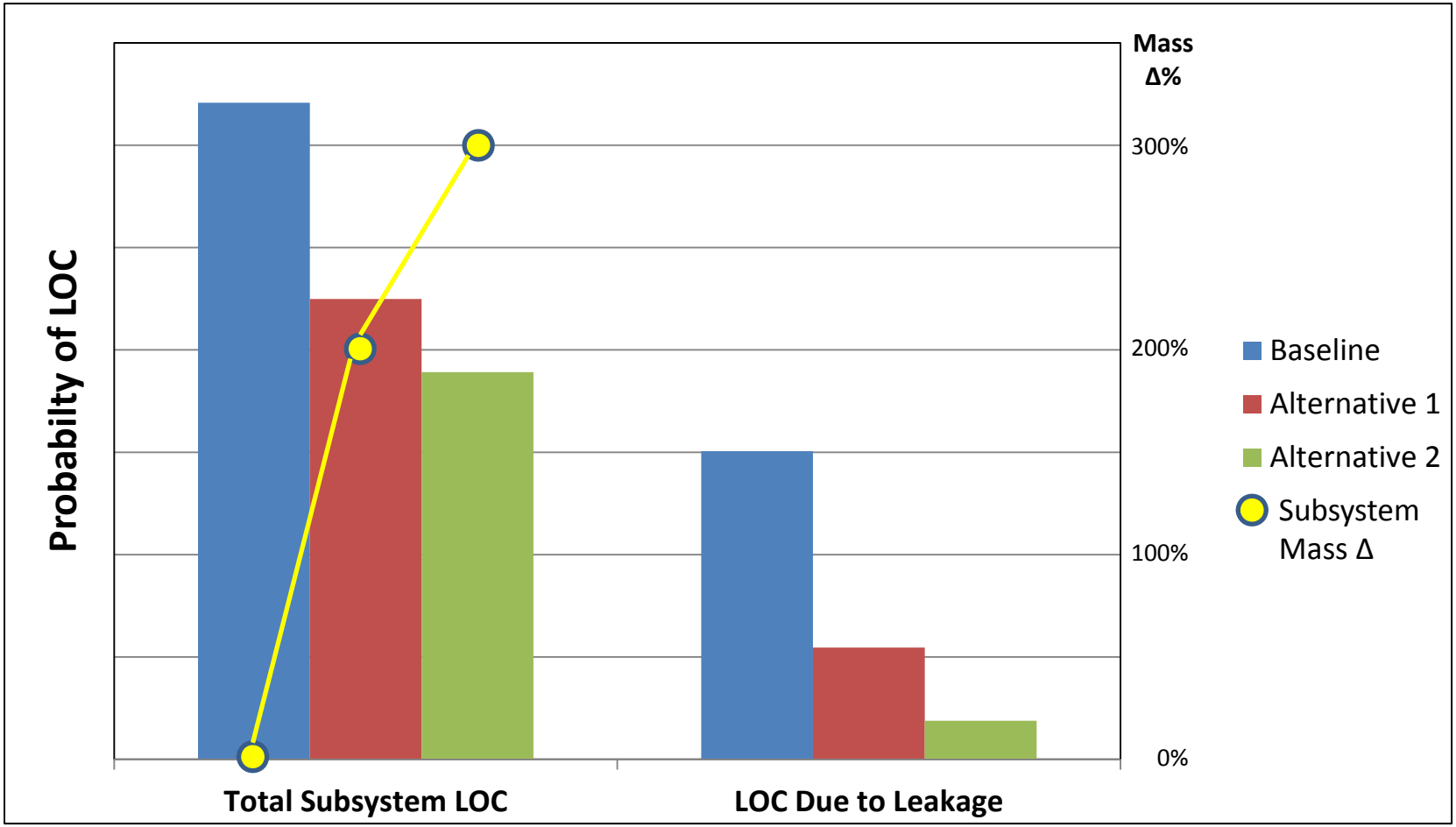
Methodology

- Methodology:
  - Develop Probabilistic Risk Assessment (PRA) models for the Baseline and Alternative Designs
    - Concentrated on fault trees for the major in-space phases of the mission
  - Determine the probability of LOC & LOM_O for each design alternative

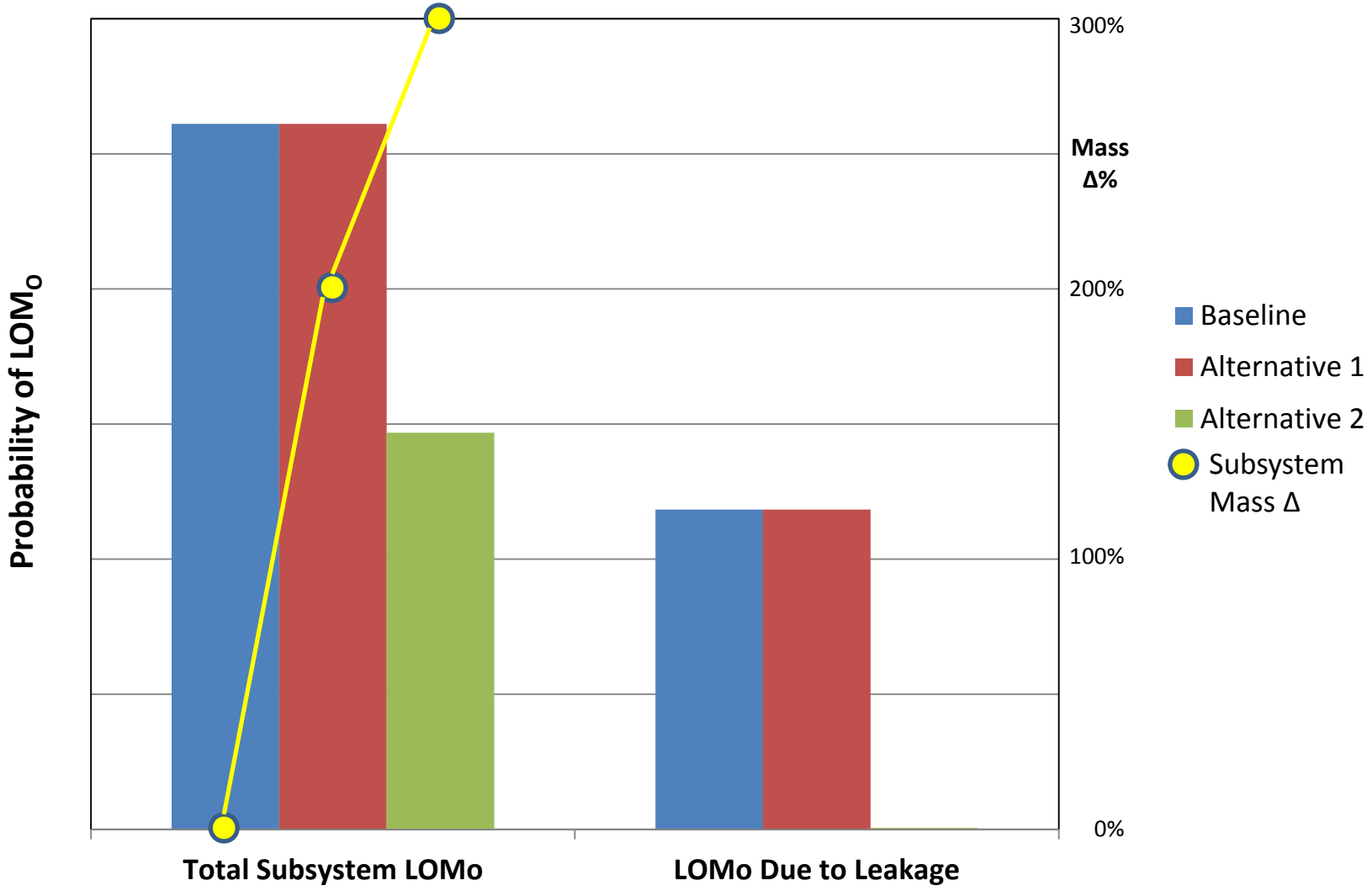
Key Assumptions

- Complete loss of a critical subsystem function was considered LOC.
- Loss of key component pairs result in loss of critical subsystem function.
- Loss of all but 1 critical component combination (or its supporting components) for a particular critical subsystem function will result in LOM_O – i.e., one failure away from LOC.
- Leakage of a single component will result in LOM_O for the Baseline and Alternative 1
- Common Cause Failure (CCF) accounted for in the model.
- Principle failure modes of interest included leakage (internal to system), fails to open on demand, and inadvertent closure for valves
- Plumbing and valve external leakage was not modeled (low probability of occurrence)
- Control electronics and electrical power not modeled for this trade study.
- Failure data used in fault tree quantification primarily from the following sources:
  - Shuttle Program PRA Iteration 3.3 (NASA/SAIC)
  - Lockheed Martin CEV-S-010
  - Generic Industry Sources (NPRD)

Results – Probability of LOC



Results – Probability of LOM_O



Conclusions

- Alternative 1 provides significant improvement in the LOC risk
  - However, no improvement to LOM_O risk
  - Alternative 2 adds additional LOC improvement to LOC risk, and all but eliminates it from LOM_O consideration
- Leakage responsible for ~45% of the LOC & LOM_O risk
  - Determined another single assembly within the subsystem was the main cause of the remaining risk
    - Risk mostly driven by a single component type!
    - Surprise to NASA engineering

Summary

- Presented a trade study example of Risk-Informed Design
- NASA engineering used results to influence design.
  - Offending component of the unexpected risk removed from the design and replaced with different design
- Probability of LOC/LOM for this subsystem still in trade against mass/schedule impact